YEARBOOK OF INTERNATIONAL & EUROPEAN CRIMINAL AND PROCEDURAL LAW
Vol.2, 2023 Article 12

Thoughts for the acquisition and use of computer evidence during investigative practice in criminal law

Megan Rafferty

DOI:10.5281/zenodo.10687551

Recommended Citation

Rafferty, M. (2023). Thoughts for the acquisition and use of computer evidence during investigative practice in criminal law. *Yearbook of International & European Criminal and Procedural Law, vol.2,* 546-571, Article 12

Available at: https://yiecpl.free.nf/index.php/yiecpl/issue/current

Thoughts for the acquisition and use of computer evidence during investigative practice in criminal law

DOI:10.5281/zenodo.10687551

Megan Rafferty, Attorney at Law, US

Abstract: The aim of this paper is to give a concrete system of logical thought on how digital evidence is acquired, its use, the related problems, the lack of an international, European and often even domestic framework with regards to non only the purchase but also the use in investigation practice. The continuous high leap in technology is a moment of crisis for cybercrimes and for the protection of fundamental principles. Computer evidence as investigation evidence is part of a reality of every system of prosecutor's offices, judicial police at national, European and international level. The problems still open as well as the solutions to fill the gaps in this regard.

Keywords: investigative evidence; cybercrimes; digital evidence; digital search and seizure; impact on fundamental principles; computer evidence.

Introduction

The continuous evolutionary path of technology and its inclusion in human life as a phenomenon of geographical, political, socio-cultural, economic analysis and above all the diffusion of smartphones have seen an endless evolution in use in developing countries and in those experiencing absolute poverty and illiteracy.

Technological tools through continuous aggressive marketing policies of brands as well as the marketing of innovative products and the evolution of the web and mobile telephony have produced transformations that are difficult for a human being to imagine.

The relation between smartphones and connection has also resulted in various findings regarding the indifference of legislators and supranational bodies towards the impact of technology and the prerogatives of the person. Collection of sensitive data, big data, tracking of user positions, archiving of commercial information, credentials disseminated in digital places with effective technologies and the revelation of a real offensive capacity of online criminal conduct. The web is a consensus of forums where various actors freely act towards vulnerable targets who are exposed to the action of cybercriminals and every hacker.

The history of recognition of the transnationality of cybercrimes dates back to the Budapest Convention of 2001 (Wicki-Bircher, 2020)[1] and the second additional protocol of the Convention of 2 February 2021[2] as an awareness of the attempt to achieve a balanced discipline in the face of the continuous challenges of technology.

The everyday digitalism of cyberspaces without territorial boundaries creates challenges in digital places with global communities that are disposed to perpetually evolving technological means.

The computing device in various forms of mobile or personal computer is welcomed to every modern society even to those that do not have water to drink thus recording reports of assault on personal property. There is an insufficiency in global governance that pushes the various national and supranational legislatures to try to legislate in the area of rights involved in interactions and in supranational principles of a treaty nature.

A conceptual line in which every legislator moves does not actually exist. The individual principles that unite legislative action at a substantive and procedural level are elements that resist various legal principles of primary rank and in the face of the new needs that progressive technological evolution imposes

1Cybercrime Convention, opened for signature in Budapest on 23 November 2001 and entered into force on 1 July 2004.

2https://www.coe.int/en/web/cybercrime/second-additional-protocol

to require the preservation of evidence parallel to the system of guarantees.

Within this very complex scenario, full of conflicting areas, this work is oriented to try to outline thoughts in the face of the claims of completeness and reflection of insights that provide clear and definitive solutions.

Web as an IT tool. The role of cybercrimes

For cybercrimes on the web, possible "solutions" have been found by the national legislator who has tried to provide ideas for comparison and security through the preservation of original data as well as the adoption of technologies aimed at preventing the alteration of the same data (Bermanns, 2022).

The search for proof for these crimes as well as for every criminal crime becomes a main tool for the repression of cybercrimes which dynamically and changeably calls the reference category, i.e. the technology of science which attributes a decisive role to every update of a permanent nature in guidelines and best practices also in fields that perform in a determined manner at an objective and causal level as well as at the subjective level of a predictive nature. The common thread is found in a very dynamic and technological field of action that binds and connects the principles known by legal practitioners.

The choices of criteria in criminal investigations do not deviate from the legal tradition and the concrete consequences produce an effective formation of evidence for criminal investigations even if different from the trial venue and the typical trial one, suggesting a sort of innovative oxymoron for investigative evidence.

Restructuring data for computer searches

For searches, the best practice for achieving the typical result and within the regulatory limits is the means for seeking proof that profiles are present, innovative and original to guarantee the integrity, genuineness of the original data and the prevention of own alteration.

Thus it moves from interpretative doubts and uncertainties of an operational nature given that the legislator refers to the acquisition of data and documents with regards to (immaterial) bits. Data that the standard refers to and that it preserves in an original way, i.e. data in the acquisition phase that are not altered and not their relevant device.

(Follows): The data

The data as bits structured in files or metafiles form a document that has an autonomous nature and which is allocated to a specific folder as storage and available to the user as well as to

the data packages that pertain to processes navigation and connectivity. The restructuring and action is carried out by the device which returns a precise picture of human action as an object of investigation. Data that is analyzed in a manner combined with the target file and which provides elements that allow restructuring to an objective profile such as a psychological trait in terms of voluntariness and awareness of action. Thus, a statement is highlighted where the psychological element of the crime manifests in a phenomenal way the location of the sphere of awareness and the voluntariness of the action as an event, excluding however the intent which is accidental.

The execution of data acquisition and analysis operations undergoes, on an argumentative level typical of the humanistic disciplines, a peculiar demonstration of the evocation of an exact mathematical demonstration as a possible achievement of the certainty that the action is aware of the sequence of actions revealing the agent's intention.

(Follows): Securitization

The custody and conservation of original data as a guarantee of the acquisition phase is noted in the chain of custody where it is noted in detail in the sequence of operations carried out and with an indication of the subjects in the procedural moment which

ends with securitization as a sequence of operations that they aim to prevent the alteration of the recovery procedure and the related change in the loss of control of the original owner (Bachmaier Winter, Ruggeri, 2022).

The acquisition operations according to the exposed sequence allow the affirmation of a use of software that is adequate to the technological standards as recognized for the purpose of the verification at trial level of the reliability of the source of evidence through the dialectical method that is attentive to the analysis of the question and which emerges from the constituted singularity of the fact that is carried out in a material way during the investigation phase and on the acquisition method with defensive and demolitive purposes in the conservation of an original data and its own alteration as a consequence of erroneous human action.

After the completion of the search operations and the seizure of the expert personnel carrying out the investigations, the outcome constitutes a closed ecosystem which must be communicated to the judge through a witness examination and the examination of the consultant. Outside this communication channel, the judge produces demolition knowledge of a finalized nature and remains attentive to the relationship of failure to comply with the obligations of inalterability and conservation.

In the anticipated moment of the investigations, the criminal evidence becomes a simple phase step that the evidence naturally places in the debate phase, definitively suggesting the investigative evidence, revealing that the judge's real ability is the evaluation of a technological data in the substantial independence of the decision, thus establishing the specialized operator of each judicial police, the technical consultants and the experts as technical body.

This is a question that is in analogy with scientific, technological knowledge which then depends on the judge who is in the evolutionary step of computer science with a decisive way in other fields of science as a claim to specialist know-how on the part of each prosecutor and of the judge who is faced with the solution of the measure of adequate knowledge in the matter which allows the production of scientific, specialized knowledge which precedes and determines the decision to continue.

Another path is sought in the possibility of conviction based on erroneous or unreliable scientific knowledge and the possibility of escaping from the responsibility of the concern that the technique used by the agent through technology and the double traceability of the fact of the passage from the suspect to the accused, leading thus towards acquittal.

The investigative action is multiple and oscillates between the stress it places on the execution of the operations that are called

necessary and the attention of the moment of the permanent update to which it refers.

The operator's documentation is detailed, concise and essential and contains information relating to the software used to extract image clones from the device's memory as a mention of the upgrade, the release that is available at the time the operations are carried out.

Videographic reproduction is appropriate for operations. Documentation via video concerns moments that require the active participation of each suspect as a problematic issue due to the potential conflict in areas that are occupied at a constitutional level (nemo tenetur se detegere). The conflicting interests and the principles of sacrifice and proportionality move through the jurisprudence evolved are sensitive according to judges at a supranational level.

Removing security measures and accessing the device

The strict qualification of the device and the material container of the data is relevant for each crime or body of crime in the strict sense and in the consideration of the need for material apprehension which also poses the related problems: the correct solution which influences the verification of the forcing of the access, i.e. the relative removal of security measures that protect the device from intrusion of a biometric, alphanumeric, double

factor and similar nature. Another path concerns the effects of turning on the relevant device that each judicial police controls, monitors the relevant content in the active connection of the device to the web and involves the relative updating of data and the relative substantial change of the same.

The problems with potential way of obligations imposed by the legislator regulate the computer search and ensure the conservation of the original data to the relative extent of operations that involve the alteration of the data themselves. The technical evaluation capacity puts the cases before the preliminary development of the device and software that are available by promptly evaluating the access that is inevitable and the operation becomes deferrable and capable of fulfilling any conservative obligation.

The relevance of the distinction of a repeatable or not act

The repeatability of an assessment comes erroneously in relation to legitimacy through national and/or transnational jurisprudence. It is understood that the data stored on a computer medium including the memory of a mobile phone is not a unique technical element and it is not mandatory to adopt acquisition methods suitable for guaranteeing the computer data and as a consequence of the failure to adopt such methods. The unusability of the related evidentiary acquisition results by

concretely evaluating any alterations from the original data and the relative correspondence with the extracted ones.

Extracting a clone copy is not an element of evaluation which can have an unrepeatable character and which participates in a technical operation, remaining in a unique way the problem of conservation of the original data and the extracted data, thus deriving from the usability of the participation of the suspect, excluding the usability of the relevant data and undermining the acquisition process through the correspondence of the original data.

Within this context we note a critical scenario that due to human error the original data can be irremediable and modified, compromising thus its conservation. The original data is intact and does not correspond to the cloned data.

The need to choose the technological path accesses the device which bypasses any protection and security measure and without at this point the collaboration of the suspect for the extraction of the clone copy and the overall data, including the navigation and connectivity by asking for verification of the process itself and the eventualities that occur.

An answer is given to the irremediable problem that compromises the original data of the relative error which can be fatal for a criminal proceeding without imagining the relative recovery and even partial use of the individual elements that are

part of the crisis of originality.

The original data undermines the correspondence of the clone copy and the judge thus repeats the technical operation that the device is available as an appropriate path that opens the way to an important reflection considering that the legislator shows that he does not appreciate the seizure of the device of an electronic nature and the return after the extraction of the clone copy, increasing the functionality of the devices in the indirect and/or direct storage of enormous quantities of varied types connected with the crime which proceeds, thus pushing many times the supranational and national jurisprudence regarding the return of the smartphone to the owner after the forensic copy phase has been concluded, specifying the motivation for the investigative need and also the need to maintain the bond of the asset, excluding the incorrectness of the extraction of the clone copy which places the basis for return as an express denial.

The return of the device to the person entitled by ascertaining the non-correspondence of the relative clone copy to its original and due to the defect of the acquisition procedure ascertains in a phenomenal and repeatable way the judge to make the device available in a legal and unreliable way given the data has been thus modified as a whole.

Thus the principle of reasonableness is sacrificed to that of proportionality of the acquisition in front of the principles of a

necessary verification of the facts of criminal relevance which preserves non-dispersion of legitimately acquired evidence. This is a technical definition of assessment and the real capacity for evaluation of the fair and effective criminal process.

Integration of data and related device. Double traceability, absolute and fundamental principles

A certain question is whether the obligation to integrate the data extends to the relevant device? The evidence, even negative, of the principle of indispensability of the prerogatives that concern the person in a dissimilar way, removes the fixed obstacles that hinder the execution of an ordinary search.

The continuous evolutionary interest of the cyber world and the conscious real extent of the long-standing and continuously evolving global change leads to tests of resistance of the traditional legal principles of new digital relations.

The connection of man to the web, the abstraction of the traditional phenomenal perception of crime in the context of digital relationships, the depersonalization of the target and the action of its sequences and the extent of cybernetic security attacks in the various articulations are open debates relating to the principles of the fundamental charters and related rights both at a national and supranational level. In a global context of new technologies, the morphology of the progressive absolute

change is included in the fundamental principles[3].

We remember Art. 15 of the Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002, relating to the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC of the European Parliament and of the Council, of 25 November 2009[4] read in light of Articles 7, 8 and 11 and Art. 52, par. 1 of the Charter of the Fundamental Rights of the European Union (Peers and others, 2021; Radoniewicz, 2021) which provide for national legislation with the aim of combating serious crime and preventing serious threats to public security, as well as the protection of public safety and security, the even limited, renewable, targeted conservation of the objective and non-discriminatory elements of data relating to traffic and the location of electronic communications means, the generalized conservation of IP addresses that are attributed to the connection of the identity civil rights of users and means of electronic communication for a limited and necessary period. Thus the balance appears to be proportionate with regard to the purposes and the precise substantive and procedural conditions of the actual guarantees

3CJEU, C-140/20, Commissioner of An Garda Síochána of 5 April 2022, ECLI:EU:C:2022:942, not yet published.

4Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37-47.

that are in favor of the interested parties against the risk of the related abuses, certainly legitimate for the use of the injunction addressed to communication service providers of electronic systems to proceed for a certain period with the rapid preservation of traffic and location data, thus disposing people who are different, suspected to verify a serious threat to public security, and committed an act of serious crime by having contact with the victim and the electronic means of communication as requirements of independence and impartiality.

Within this context the Court of Justice of the European Union in the recent case C-401/19 of 26 April 2022[5] gave extension of liability to sharing service providers for the violation of copyright and limitation of the right to free expression of thought. It is pronounced regarding:

"(…) the comment on the legitimacy of Art. 17 of Directive 2019/790 on copyright and related rights in the digital single market, which provides that providers of online content sharing services are directly liable in the event that materials protected by copyright are uploaded illegally by its users (…)".

It was contested (from Poland) that the regime provided for by paragraph 4 of Art. 17, according to which service providers, in order to be exempt from liability, have the obligation to make maximum efforts, on the one hand, to ensure that specific protected content for which the rights holders have provided the relevant information is not available and necessary and, on the

5CJEU, C-401/19, Poland v. Parliament and Council of 26 April 2022, ECLI:EU:C:2022:297, not yet published.

other hand, to prevent the protected contents subject to a sufficiently motivated report by such owners from being uploaded in the future, forces the service providers themselves to carry out preventive surveillance through automatic content filtering, with serious prejudice of freedom of expression and information. This effectively entails a limitation of the exercise of the right to freedom of expression and information of the users of such sharing services. Additionally, this limitation must be considered legitimate and justified, according to the criteria provided for by Art. 52 of the Nice Charter, by virtue of the complex regime provided for by Art. 17, including subsequent paragraphs (from 7 to 10), containing corrections that aim to ensure that the limitation of freedom of expression is expressly provided for by law in its contents and methods, and must be necessary and proportionate to the counter-interest that it is intended to protect. In this case, we refer to intellectual property[6].

The European Commission. The Strengthened Code of Practice on Disinformation (2022): some limitations

The European Commission through the Strengthened Code of Practice on Disinformation 2022 adopted on 16 June 2022[7] strengthens the code of good practices for the online platform,

6CJEU, C-401/19, Poland v. Parliament and Council of 26 April 2022, op. cit.

7https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

the associations of the relevant category as well as operators in the advertising sector who combat disinformation to improve online policies that are adopted before 2018.

The 2018 code, with 16 signatories stated:

"(…) commitments based on self-regulation, inherent to the scrutiny of advertisers, the integrity of their services, the empowerment of consumers, as well as fact-checkers and researchers, the version strengthened, with 34 signatories, 44 commitments and 127 specific measures, refers to the forms of co-regulation to which very large online platforms are subject in the framework of the Digital Service Act" in order to increase the incisiveness of the measures and transparency of political and thematic advertising, as well as ensuring complete surveillance of current and emerging manipulative behaviors".

It is planned to expand and strengthen the tools that allow users to identify and report false or misleading content, establish a solid monitoring and communication framework, establish a center for transparency and create a permanent task force for the evolution and adaptation of the code. Overall, it is based on the common consideration of the increased aggressiveness and harmfulness of cybercriminal conduct to combat what is necessary to adopt measures whose specialty is essentially found in the compression of the extension of fundamental rights.

Cybercrimes with double traceability of the fact. Identification of the device and the offender

The new jurists in all guises should demand dynamic behavior as an expression of a punitive law that objectively orients itself in the face of the rampant forms of cybercrime. The tension of

the double traceability through the agent under an objective-causalistic and subjective-malicious profile where the crime in a cybernetic environment remains in criminal law as a human act that commits a guilty will be attributing to each agent, to his own conscious and voluntary conduct. Thus, intentional, unjustified access to websites is necessary in cases of child pornography, confirming the trend of controlled limitation of criminal policy choice rights.

At a procedural level, the technological investigation evaluates connectivity through a tool used to commit the crime and the related device of an identification system through matching the combination of use between user and IP address.

The verification of a crime identified through the device coincides with the identification of the perpetrator of the crime not in an isolated way but through the investigation of cybercrimes with a technological and traditional way of investigation which is outdated. The issues are not random but essential checks in criminal law. The double traceability of the fact to the agent on an objective and subjective level such as an investigation that stops the identification of the IP and through the search of log files as a user which is associated, is incomplete to the extent that it is identified with the owner of the user.

The use of an IMEI code on the device is associated with the user as a decisive issue for the use of the device and where the IMEI code is associated with criminal liability. The related investigations aim to define in a linear way the criminal responsibility for a cyber crime by using technology and the traditional verification of the circumstances, thus identifying the subject in multi-subjective cases who has carried out the voluntary action and the realization of an event that considers and prohibits the incriminating case. It is necessary to carry out the identification of the contacts from the printouts relating to the user, continuing with the control of the circumstances that occur through the activated cells, thus carrying out a preliminary verification check and understanding for the user owner the subjective target of the revelation aimed at an investigation.

After the identification of the subject, the verification connection that serves a domestic network of an open nature and/or protected by people that is made up of the family unit that frequents the place served by the network will be examined. Thus, material access and the moment of the IT search create various questions such as when do you change your smartphone and for what reason? Are the data relevant for migration operations so dispersed? Are device searches so out of use?

The device of the material in question will have access to a series of information that is useful in directing the investigation

into the correct subject and thus digital places allow a quick way to understand that the owner of a user is also the user of a device such as a right target. The formation of the key of custody, the extraction of the clone copy, the overall collection and use of the data and the restructuring continue at a logical and chronological point in time. The legislation of the investigative action in a procedure that should ascertain criminal responsibility attributes the relevant fact to a specific subject as a crime in question by demonstrating the realization of an event contemplated in the incriminating case and as a consequence of his own action. Every reasonable doubt is a parameter of a code nature which broadens the extension of the principle of double traceability. The decalogue of operations refers to a categorical and exhaustive way that serves to understand the direction and fluidity of the investigation carried out in this regard.

Web 3 and metaverses. Extension of double traceability. What future do they have?

The possibility of successful investigations in an area where technology evolves rapidly and in favor of cybercriminals considering that the double traceability goes beyond any reasonable doubt, establishes a procedural certainty of the responsibility of the accused.

The favorable outcome of an investigation is considered as a direction in which technology rapidly evolves, thus eluding the tracking of the concealment of digital identity (anonymization, false identity, IP masking). It is concerned that the person who directs the investigation, also called to identify a single subject, is part of a broad group of actors such as wi fi, transfer, sharing of access credentials, open networks, adding the ordinary and extraordinary phases of use that in an accessible way it puts the web in various forms (surface, deep, dark web): VPN, easily accessible proxy servers, NAT, hacked computers, fake identity generator, thus making the related ongoing investigation useless and risky.

The forms of cloud storage are inaccessible since they are protected by advanced encryption enabling the obstacle of a final step of the investigation to the extent that it prevents access, the acquisition which exemplifies the presence and certainty of the procedural phase in the exchange of files relating to child pornography content, cloud storage which is inaccessible and which frustrates the investigation. The downloaded files are available files that are allocated to the cloud. Not accessing a platform with one's IP is visible to an identity that masks the IP via VPN and one's registration for the email service as well as for social networks, various services, fictitious telephone numbers, emails, false identities, intelligence

artificial and so on.

Moving from voluntary to mandatory disclosure according to the second additional protocol of the Budapest Convention which obliged ISPs to provide the judicial authorities with the relevant information, including cross-border information, relating to the identities of users who are registered (subscriber data), is an attempt to road that reacts to the phenomenon of anonymization and the solution to the problem of the large number of messaging service providers and the proliferation that is uncontrolled in multifunctional platforms and due to the transformation of the web and progressive decentralization. Web step 3 is characterized by the lack of a provider who is focused on any effort that has to do with identification.

The most well-known ISPs look at the compliants who in the past the performance orders have lacked the KYC procedure at a very high level, thus restoring the certainty of the identification of the subscriber and the user of the service.

The digital world continues and represents a challenge in the field of investigations before operators in the field of the metaverse, of the metaverses organized in digital places articulate a virtual reality that has to do with information obligations that are imposed on the relevant exchanges.

The home address, the complete registration of a person, the telephone number, the credit card codes are ways of creating an

identity that is certainly findable but false and unrealistic. Cybercrime investigations are aware of a technological evolution that contributes to investigative techniques and useful, effective investigations which must certainly be restricted both at a domestic, European and international level.

Concluding remarks

The constantly evolving technological "attack" on an action plan for cybercriminals at an investigative level are points of priority, analysis but also of change of this regime. The line of argument considers predictive algorithms to determine certainty sentences in a way that complies with a regulatory model of guarantees and with a subject whose consequences are of a conscious nature.

Criminal evidence is part of a research process, conservation of the relevant evidence and a level of technology that characterizes the facts of each investigation. The principle of double traceability in a reasonable manner does not undergo expansions of the prerogatives of a subjective nature which reveals data that are interesting.

The limitations of the principles in international law operates on the level of safeguard policies in the order of public security through the imposition of obligations on third parties that influence and create a decisive role in the information moment

in the expansions of the principles of the same supranational sources that aim to strengthen rights and guarantees in the context of substantive and procedural criminal law, leaving the nature of the crime in the background.

The attribution of the device (matching), the intrusion into people's digital places, the apps installed and the methods of use, the examination concerning the connectivity and the relative navigation, the study of the storage, recourse to the cloud are some of the demonstrations of the voluntariness of the action, of the overall elaboration of the evidentiary process subjected to the examination of each judge debated with a dialectical method by the parties, thus resulting in a linear, unambiguous manner in the determined reconstruction of the affirmation of the responsibility of procedural certainty.

The investigative evidence, the anticipation of the investigation phase, the acquisition of the future decision with an exclusive way of the acquisition methods draws the sources of evidence, the effectiveness of the defense rights thus turning a look at the technological evolution of precise obligations of the violation entails an irremediable invalidation of the punitive claim.

Technology is not considered as an optional behavior. It pervades the daily life of human action in a way that is direct to human relationships and which determines behaviors that are not considered in an extraordinary or isolated way. These are

new scenarios that are linked to technological evolution that places challenges before an indispensable front where the exact opposite of indifference to various sectors in this regard shows the daily logic of our times.

References

Bachmaier Winter, L., Ruggeri, S. (2022). *Investigating and preventing crime in the digital era: New safeguards, new rights.* ed. Springer, Berlin, 125ss.

Bermanns, G. (2022). Strengthening trust and security in the EU cybersecurity policy. *Yearbook of European Union and Comparative Law, vol. 1 (1),* 45ss.

Peers, S. et al. (eds.), *The EU Charter of Fundamental Rights, A commentary.* Hart Publishing, Nomos, C.H. Beck, Oxford & Oregon, Portland.

Radoniewicz, F. (2021). Cybsersecurity in the European Union law. In K. Chałubińska-Jentkiericz, D. Radoniewicz, T. Zieleński, *Cybersecurity in Poland. Legal aspects.* ed. Springer, Berlin, 2021, 76ss.

Wicki-Bircher, D. (2020). The Budapest Convention and the general data protection regulation: Acting in concern to curb cybercrime?. *International Cybersecurity Law Review, 1,* 65ss.